

4001.0.0 NOTICE OF PRIVACY PRACTICES

4001.0.1 This establishes instructions to all DHS offices, facilities, programs and workforce members (entities) regarding the provision of a Notice of Privacy Practices to all clients.

4001.0.2 This rule applies to all DHS employees. DHS offices, facilities, programs and workforce members are directed to follow all applicable policies and procedures found in the Health Insurance Portability and Accountability Act (HIPAA) Policies and Procedures Manual. Failure to comply with this rule and its reference documents will result in disciplinary sanctions as defined by the HIPAA Policy and Procedures Manual and in Policy 1084, Employee Discipline.

4001.1.0 Authority

HIPAA Standards for Privacy of Individually Identifiable Health Information 45 CFR Part 164 Section 164.520 Notice of Privacy Practices for Protected Health Information. To issue instructions to all DHS offices, facilities, programs and workforce members (“entities”) regarding the Department’s obligations relating to the implementation of HIPAA, 42 U.S.C. §§ 1320d-1329d-8, and regulations promulgated thereunder, 45 CFR Parts 160 and 164.

4001.2.0 Definitions

4001.2.1 Protected Health Information (PHI) - is health information which:

- A. Identifies the individual or offers a reasonable basis for identification
- B. Is created or received by a covered entity or an employer; and
- C. Relates to past, present, or future
 - 1. Physical or mental health or condition
 - 2. Provision of health care or
 - 3. Payment for health care
- D. AND has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form. To be PHI, the information must:
 - 1. Relate to a person’s physical or mental health, the provision of health care, or the payment of healthcare
 - 2. Identify, or could be used to identify, the person who is the subject of the information
 - 3. Be created or received by a covered entity
 - 4. Be transmitted or maintained in any form or medium
 - Electronic
 - Written, or
 - Oral

- 4001.2.2 Workforce Members - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DHS, its offices, programs or facilities, is under the direct control of DHS, regardless of whether they are paid by the entity.
- 4001.2.3 Covered Entity (CE) – a health plan that provides, or pays the cost of medical care, a health care clearinghouse, or a health care provider.
- 4001.2.4 Treatment, Payment and Operations (TPO):
- A. Treatment – the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
 - B. Payment – activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
 - C. Operations – functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

4001.3.0 Policy

An individual has a right to adequate notice of the uses and disclosures of his/her PHI that may be made by or on behalf of a CE, and of the individual's rights and the CE's legal duties with respect to his/her PHI.

4001.4.0 Notice of Primacy Practices

- 4001.4.1 DHS will make available a copy of the DHS Pub 407, Notice of Privacy Practices, to any client applying for or receiving services from DHS.
- 4001.4.2 The Notice of Privacy Practices shall contain all information required under federal regulations regarding the notice of privacy practices for protected health information under HIPAA.
- 4001.4.3 Where DHS is a CE, DHS will seek to acquire a signed DHS Notice of Privacy Practices Acknowledgement of Receipt, from each client.
- 4001.4.4 Provision of Notice: Department facilities and programs must provide individuals with the notice, and obtain the individual's written acknowledgement of receipt, or document attempts to obtain such acknowledgement, no later than the date of the first service delivery. The receipt of acknowledgement will be maintained in the client file or casehead file. Additionally, the notice in effect (original notice or any subsequent revisions) must be prominently posted at each DHS County Office and copies must be available for individuals at the County Office or upon request. .

- 4001.4.5 The privacy notice will also be posted on the DHS website and available electronically from the website.
- 4001.4.6 Revisions to Notice: DHS will promptly revise and distribute the privacy notice whenever there is a material change to the uses or disclosures, the individual's rights, the CE's legal duties, or other privacy practices described in the notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.
- 4001.4.7 Documentation Requirements: DHS will retain copies of notices issued for a period of at least six years from the later of the date of creation or the last effective date and each facility and program will retain documentation of individuals acknowledgement of receipt, or refusal to acknowledge receipt, of the privacy notice for a period of at least six years.
- 4001.5.0 Attachments to Policy**
- Notice of Privacy Practices Acknowledgement of Receipt Form
 - Notice of Privacy Practices
- 4001.6.0 Originating Section/Department Contact**
- Office of Chief Counsel
Donaghey Plaza South
P. O. Box 1437, Slot S260
Little Rock, AR 72203-1437
Telephone: (501) 682-8934

4004.0.0 MITIGATION OF VIOLATIONS OF PRIVACY RIGHTS

4004.1.0 Duty to mitigate violations of privacy rights guaranteed under HIPAA

As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Human Services (DHS) shall mitigate any known harmful effect(s) of uses or disclosures of Protected Health Information made by DHS or its business associates in violation of HIPAA or DHS policy related to privacy rights granted by HIPAA. (45 CFR § 164.530 (f))

4004.2.0 Mitigation

Mitigation means taking all appropriate actions listed below if a DHS Client's HIPAA privacy rights have been violated.

- A. Notifying any unintended or unauthorized recipient(s) of Protected Health Information (including by e-mail or fax) and requesting them to disregard, keep confidential, not reveal, and discreetly dispose of said information.
- B. Investigating the causes of the disclosure.
- C. Taking corrective action, including:
 - 1. Sanctioning personnel for unauthorized use or disclosure of client information in accordance with DHS Policy.
 - 2. Training or retraining as necessary.
 - 3. Correcting faulty processes.

4004.3.0 Originating Section/Department Contact

Office of Chief Counsel
Donaghey Plaza South
P. O. Box 1437, Slot S260
Little Rock, AR 72203-1437
Telephone: (501) 682-8934

4005.0.0 DHS PROTECTED HEALTH INFORMATION COMPLAINT PROCEDURE

This policy establishes Department of Human Services (DHS) procedures to complain to DHS or to the Secretary of the Department of Health and Human Services regarding violations of privacy rights granted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Rules found at 45 CFR Parts 160 and 164. This policy is applicable to all DHS clients and their legal representatives.

4005.1.0 Privacy Rights Under HIPAA Generally

DHS clients and their legal representatives (DHS clients) have certain rights guaranteed under HIPAA pertaining to the safeguarding of the privacy of their Protected Health Information (PHI) retained by or created by DHS and its agencies. The legal representatives of DHS clients may exercise these rights on behalf of the DHS client they represent. References to clients therefore includes legal representatives of clients. These rights generally include the following:

- 4005.1.1 Use and disclosure of a client's PHI by DHS and its agencies will be limited to those who have a need to know, and the amount of PHI disclosed will be the minimum necessary to accomplish the purpose of the communication.
- 4005.1.2 Clients have the right to request restrictions on the use and disclosure of their PHI during activities of treatment, payment of claims, and operations.
- 4005.1.3 Clients may request DHS to send their information to a certain address and package it in a certain way or send it by a certain medium. (See DHS 4008)
- 4005.1.4 Clients have the right to inspect and copy their PHI.
- 4005.1.5 Clients have the right to request DHS amend their patient information.
- 4005.1.6 Clients have the right to request and receive an accounting of disclosures of their PHI. (See DHS 4001)
- 4005.1.7 Clients have the right to receive a written copy of the DHS Notice of Privacy Practices. (See DHS Pub 407)
- 4005.1.8 Clients have the right to request that DHS not disclose their PHI to certain parties.
- 4005.1.9 Clients have the right to file complaints regarding violations by DHS of their privacy rights granted to them and created by HIPAA.
- 4005.1.10 Clients have the right to require that DHS refrain from any activity that may intimidate, threaten, coerce, discriminate against them for exercising their rights under HIPAA.

4005.2.0 Client's Right to File a Complaint for Violation of HIPAA Privacy Rights

Any client or legal representative of a client may complain to DHS or the United States Department of Health and Human (DHHS) services of violations by DHS of the client's privacy rights granted by HIPAA.

4005.3.0 Requirements for Filing a Complaint

All Complaints must meet the following requirements:

- A. A Complaint must be made in writing, either on paper or electronically.

The Complainant may use the DHS Complaint form for convenience or may personally compose his or her complaint in his or her own words. DHS will recognize complaints filed in either form.
- B. A Complaint must name the covered entity that is subject of the complaint and describe the acts or omissions believed to be in violation of HIPAA privacy rights.
- C. A Complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by either DHS or DHHS for good cause shown.

4005.4.0 Filing the Complaint

Complaints made in accordance with the previous section may be made to the following persons:

- A. DHS Privacy Officer: (state of Arkansas)

DHS Privacy Officer
Department of Human Services
P.O. Box 1437, Mail Slot S201
Little Rock, Arkansas 72203-1437
Ph: 501-682-8650
- B. U.S. Secretary of Department of Health and Human Services (federal)

U.S. Department of Health and Human Services
Office for Civil Rights
Medical Privacy, Complaint Division
200 Independence Avenue, SW
HHH Building, Room 509H
Washington, D.C. 20201
Phone: 866-627-7748
TTY: 886-788-4989 Email: www.hhs.gov/ocr

4005.5.0 Investigating the Complaint

4005.5.1 The DHS Privacy Officer shall investigate each complaint submitted to him or her, and report his or her findings to the complainant in writing within 60 days from the date the complaint was received.

4005.5.2 The DHS Privacy Officer will document all complaints and their disposition, if any, in the Complainant's DHS file, and in a separate file for Complaints made pursuant to privacy and confidentiality rights.

4005.6.0 Originating Section/Department Contact

Office of Chief Counsel
Donaghey Plaza South
P. O. Box 1437, Slot S260
Little Rock, AR 72203-1437
Telephone: (501) 682-8934

4006.0.0 HIPAA PRIVACY REQUIREMENTS IN THE USE OF EMAIL AND FACSIMILE SERVICES

4006.1.0 Purpose

4006.1.1 Electronic mail (E-mail), Internet access, and Facsimile (Fax) services are made available to DHS staff for the purpose of facilitating the conduct of DHS business and enabling the efficient communication of information and data.

4006.1.2 These services must be used by DHS staff in a manner that conforms to all applicable state and federal laws, regulations and policies. Each DHS employee is responsible for ensuring the privacy of Protected Health Information (PHI).

4006.2.0 Email Procedures

4006.2.1 **Approved Methods of Conveyance:** All email messages, containing Protected Health Information (PHI)(as defined below) and sent by DHS staff to destinations within the state's email system, must be sent using the encrypted WebAccess email interface. Sending of email messages, containing PHI, to destinations outside the state's email system is not secure and is prohibited; such messages must be sent by Fax, employing the privacy safeguards outlined in 4006.3.0 below. Conveyance of large electronic files requires secure media sharing (password protected files on disk or CD) or conveyance by a secure transfer protocol; consult with Office of Systems & Technology for assistance.

4006.2.2 **Content Requirements:** Any E-mail message generated by DHS staff that contains PHI shall conform to the following requirements:

4006.2.3 **E-mail Subject Line:** For messages containing PHI, the subject line shall state, in whole or in part, "CONTAINS PROTECTED INFORMATION".

4006.2.4 **E-mail Addressees:** E-mail messages may be sent, copied, or forwarded *only* to those persons who have a *need to know* the patient information. Global, group, or broadcast addresses *should not be used* when sending E-mail messages that contain PHI. The purpose of this requirement is to avoid inadvertent disclosure to addressees who lack a need to know the Protected information.

4006.2.5 **E-mail Message:** At the bottom of the message the following privacy warning must be displayed: "Confidentiality Notice: The information contained in this email message and any attachment(s) is the property of the State of Arkansas and may be protected by state and federal laws governing disclosure of private information. It is intended solely for the use of the entity to whom this email is addressed. If you are not the intended recipient, you are hereby notified that reading, copying or distribution this transmission is STRICTLY PROHIBITED. The sender has not waived any applicable privilege by sending the accompanying transmission. If you have received this transmission in error, please notify the sender by return and delete the message and attachment(s) from your system."

- 4006.2.6 **Minimum necessary content:** E-mail messages containing PHI shall contain only the *minimum necessary* information to accomplish the purpose of the communication.
- 4006.2.7 **Unsecured Email Requirements:** When originating messages in the state's unsecured email system (ie. Not WebAccess), users are required to review messages, and attachments, and must expunge all information that may be defined as PHI. Such review is required not only for messages authored by the user but also for forwarded messages and all the messages in the forwarded strings.
- 4006.2.8 **User Hard Drives:** Hard drives must also be protected from PHI disclosure. Use of Personal Folders (Microsoft Outlook) creates a file on the local hard drive which may be exposed to the Internet through the use of file sharing applications (eg. Napster, Swapnut, Gnutilla, etc.) and the efforts of malicious hackers. Installation of third party file sharing applications is prohibited. DHS employees must expunge PHI from Personal Folders in their Outlook account.
- 4006.3.0 Fax Procedure**
- 4006.3.1 **Approved Methods of Conveyance:** All Fax messages, containing Protected Health Information (PHI)(as defined below) and sent by DHS staff to any destination, must be safeguarded for confidentiality and privacy in accordance with federal and state law, and must employ privacy safeguards outlined in this section. Faxes may be sent only to a specific person for whom such release has been determined to be authorized. It should be established, by prior telephone contact, that a specific person is present to receive the transmitted fax.
- 4006.3.2 **Content Requirements:** Fax messages shall utilize a cover sheet with the word CONFIDENTIAL appearing in bold letters near the top of the form. Further, all such Faxes must include a statement regarding prohibition of disclosure of identifying PHI. The statement shall read as follows:
- Prohibition of Redislosure: This information has been disclosed to you from records that are confidential. You are prohibited from using the information for other than the stated purpose; from disclosing it to any other party without the specific written consent of the person to whom it pertains; and are required to destroy the information after the stated need has been fulfilled, or as otherwise permitted by law. A general authorization for the release of medical or other information is not sufficient for this purpose.*
- 4006.4.0 Protected Health Information Defined – HIPAA (Health Insurance Portability and Accountability Act of 1996)**
- 4006.4.1 Protected Health Information (PHI) is health information which: (1) Identifies an individual or offers a reasonable basis for identification; (2) Is created or received by a covered entity or an employer; and (3) Relates to past, present, or future physical or mental health condition, provision of health care, or payment for health care; And which has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form. To be PHI, the information must (1) relate to a person's physical or mental health, the provision of health care, or the

payment of healthcare; (2) Identify, or could be used to identify, the person who is the subject of the information; (3) Be created or received by a covered entity; (4) Be transmitted or maintained in any form or medium, electronic, written, or oral.

4006.4.2 Examples of PHI: First and last names; Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code; Dates, including birth date, admission date, discharge date, date of death, all ages over 89; Telephone numbers, fax numbers, e-mail addresses; Social Security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identification numbers, serial numbers, driver's license number, license plate number; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; Full face photographic images and any comparable images; Any other unique identifying number, characteristic, or code.

4006.5.0 Discipline for Violation of Policy

Supervisors will follow DHS Policy 1084, Employee Discipline, to determine the appropriate discipline for conduct violations and imposing disciplinary actions.

4006.6.0 Department Contact

Any questions concerning this DHS policy should be directed to:

Office of Chief Counsel
Donaghey Plaza South
P. O. Box 1437, Slot S260
Little Rock, AR 72203-1437
Telephone: (501) 682-8934

4007.0.0 DE-IDENTIFIED PROTECTED HEALTH INFORMATION/FREEDOM OF INFORMATION ACT

The Department of Human Services (DHS) has established a uniform method and system for responding to requests for access to or copies of records as required under the Arkansas Freedom of Information (FOI) Act codified beginning at Ark. Code Ann. 25-19-104. As established under DHS policy DHS 1053.4.0 some information is exempt from disclosure and specifically, DHS policy 1053.4.13 exempts disclosure if “Other state and federal laws prohibit disclosure of client identifying information.” The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects disclosure of Protected Health Information or (PHI) and also necessitates the need to de-identify PHI.

4007.1.0 Definition

4007.1.1 Protected Health Information (PHI) is health information which:

- A. Identifies the individual or offers a reasonable basis for identification
- B. Is created or received by a covered entity or an employer; and
- C. Relates to past, present, or future
 - 1. Physical or mental health or condition
 - 2. Provision of health care or
 - 3. Payment for health care
- D. AND has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form. To be PHI, the information must:
 - 1. Relate to a person’s physical or mental health, the provision of health care, or the payment of healthcare
 - 2. Identify, or could be used to identify, the person who is the subject of the information
 - 3. Be created or received by a covered entity
 - 4. Be transmitted or maintained in any form or medium
 - Electronic
 - Written, or
 - Oral

4007.1.2 DHS’s policy is to de-identify PHI to meet FOI requests received by the department. This policy adheres to 45 CFR Part 164 Section 164.502 (d) and Section 164.514 (a) and (b) addressing de-identification of Protected Health Information (PHI).

4007.2.0 Definition

4007.2.1 De-identified PHI is health information from which identifiers have been removed so that the health information is no longer identifiable to any individual.

4007.2.2 Individual identifiers that would be removed or redacted to de-identify PHI include, without limitation, the following:

A. Names

All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

B. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

C. Telephone numbers

D. Fax numbers

E. Electronic mail addresses

F. Social security numbers

G. Medical record numbers

H. Health plan beneficiary numbers

I. Account numbers

J. Certificate/license numbers

K. Vehicle identifiers and serial numbers, including license plate numbers

L. Device identifiers and serial numbers

M. Web Universal Resource Locators (URL's)

N. Internet Protocol (IP) address numbers

O. Biometric identifiers, including finger and voice prints

P. Full face photographic images and any comparable images

Q. Any other unique identifying number, characteristic, or code, except as permitted to re-identify protected health information; and

4007.2.3 Once health information is properly de-identified, there no longer exists a reasonable probability the information could be used alone or in combination with other information to identify any individual who is the subject of the information.

4007.3.0 Usage

4007.3.1 PHI shall be de-identified when the source of the data request is outside of DHS operations or the source is required to comply with a FOI request.

4007.3.2 If anyone within DHS is unsure if PHI has been de-identified according to HIPAA guidelines then that person should seek approval from the DHS privacy officer.

4007.3.3 Failure to comply with this policy will result in disciplinary action as defined in Policy 1084, Employee Discipline.

4007.4.0 Department Contact

Office of Chief Counsel
Donaghey Plaza South
P. O. Box 1437, Slot S260
Little Rock, AR 72203-1437
Telephone: (501) 682-8934

4008.0.0 CONFIDENTIAL COMMUNICATIONS REQUIREMENTS

4008.1.0 Purpose

To enable Department of Human Services (DHS) clients/employees to request receiving communications of protected health information from DHS by alternative means or to an alternate locations.

4008.2.0 Authority

HIPAA Standards for Privacy of Individually Identifiable Health Information 45 CFR Part 164 Section 164.522 (b) Confidential communications requirements.

4008.3.0 Applicability

This rule applies to all DHS employees. DHS offices, facilities, programs and workforce members are directed to follow all applicable policies and procedures found in the DHS Policies and Procedures Manual. Failure to comply with this rule and its reference documents may result in disciplinary sanctions as defined in Policy 1084, Employee Discipline.

4008.4.0 Definitions

4008.4.1 Protected Health Information (PHI) is health information which:

- A. Identifies the individual or offers a reasonable basis for identification
- B. Is created or received by a covered entity or an employer; and
- C. Relates to past, present, or future
 - 1. Physical or mental health or condition
 - 2. Provision of health care or
 - 3. Payment for health care

AND has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form. To be PHI, the information must:

- A. Relate to a person's physical or mental health, the provision of health care, or the payment of healthcare
- B. Identify, or could be used to identify, the person who is the subject of the information
- C. Be created or received by a covered entity
- D. Be transmitted or maintained in any form or medium
 - Electronic
 - Written, or
 - Oral

4008.4.2 **Workforce Members** - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DHS, its offices, programs or facilities, is under the direct control of DHS, regardless of whether they are paid by the entity.

4008.4.3 **Covered Entity (CE)** – a health plan that provides, or pays the cost of, medical care, a health care clearinghouse, or a health care provider.

4008.5.0 Policy

4008.5.1 DHS must permit clients and employees to request and must accommodate reasonable requests by clients and employees to receive communications of protected health information (PHI) from DHS by alternative means or at alternative locations. Examples of such requests may include mailing PHI to an alternate address specified by the individual, transmission of such information to a specific phone number by facsimile, or transmission of such information via e-mail, etc.

4008.5.2 The Department is not required to accommodate unreasonable requests for alternate delivery of PHI. Examples of such requests may include asking for delivery of PHI by registered or certified mail, or requesting that PHI be hand carried to the client to an off-site location.

4008.6.0 Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of the organization.

A. The client/employee must request to receive PHI from DHS by alternate means or to an alternate location and must specify the preferred alternate means or location. Requests for alternate means of transmitting PHI or delivery to an alternate location may be made orally or in writing. Telephone requests for alternate delivery of PHI should have a second party confirmation of the client's identify and requested change. This may be accomplished by having another employee listening to the client's request or having the employee confirm the client's request after it is made.

1. If the request is made orally, DHS staff must document the request and ask for the client/employee's signature.
2. If the request is made by telephone or by electronic media, DHS staff must document the request and verify the identity of the requestor.
3. Documented client/employee requests for alternate means of delivery or alternate locations for delivery of PHI will be filed in the client/employee record and appropriate updates will be made to the client/employee's record (case file, medical record, electronic database, etc.).

B. Prior to sending any PHI to a client/employee, DHS staff will review the client/employee's record to confirm whether the client/employee has requested that PHI be sent by alternate means or to an alternate location.

- C. DHS will forward PHI to the client in accord with the client/employee's preferred means or location when requested or to his current mailing address, as appropriate.
- D. DHS may terminate its agreement to deliver PHI via alternate means or to an alternate location if:
 - 1. The client/employee agrees to or requests termination of the alternate delivery location or method of communication in writing or orally. DHS staff must document the request or oral agreement in the client/employee's record.
 - 2. Use of the alternative delivery location or method of communication is not effective (i.e. DHS is unable to contact the client/employee at the location or in the manner requested by the client/employee). In this instance, DHS must inform the client/employee that it is terminating its agreement to alternative means or location of delivery of PHI and provide the reason(s) for termination of the agreement.
- E. DHS must retain all documentation related to requests for alternative means of delivery of PHI or alternate delivery location for PHI for a minimum period of six years.

4008.7.0 Program Coordination

- 4008.7.1 The DHS representative handling the client/employee request for delivery of PHI by alternate means or to an alternate location will determine (with the assistance of the client/employee) the other Divisions/Offices within DHS that may hold protected health information on the individual. When affected Divisions/Offices are determined, the representative will forward a copy of the request for alternate delivery of PHI to the privacy official of each Division/Office and to the Department's Privacy Officer.
- 4008.7.2 When the client/employee terminates the request for alternate delivery of PHI, or it is determined that the alternate method of delivery is unreliable (i.e. mail has been returned, FAX machine number has been disconnected or has no FAX to receive messages, etc.), the representative will notify:
 - A. The client/employee of the termination of alternate delivery of PHI
 - B. All affected Divisions/Offices of the termination of the alternate delivery method
 - C. The Department's Privacy Officer.

4008.8.0 Originating Section/Department Contact

DHS Privacy Official
Donaghey Plaza South
P. O. Box 1437, Slot S201
Little Rock, AR 72203-1437
Telephone: (501) 682-8650

4009.0.0 USES AND DISCLOSURES OF CLIENT OR PARTICIPANT INFORMATION

4009.1.0 Purpose

The purpose of this policy is to specify requirements for authorization to disclose individually identifiable health information and to recognize the standard authorization form that must be used by all Department of Human Services (DHS) agencies that serve clients. Any of the following DHS agencies that serve clients must comply with this policy: covered health care components, internal business associates, and non-covered health care components that maintain individually identifiable health information.

4009.2.0 Background

Each DHS agency shall make reasonable efforts to protect individually identifying health information maintained by that agency. Therefore, no DHS agency shall disclose, or be required to disclose, in individually identifiable format, information about any such individual without that individual's (or their personal representative's) explicit authorization, unless for specifically enumerated purposes such as emergency treatment, public health, law enforcement, audit/oversight purposes, or unless state or federal law allows specific disclosures.

4009.3.0 Policy

4009.3.1 General – Individual Authorization

4009.3.1.1 DHS shall not use or disclose any information about a client or participant of DHS programs or services without a signed authorization for release of that information from the individual, or the individual's personal representative, unless authorized by this policy, or as otherwise required by state or federal law.

4009.3.1.2 DHS requires use of DHS Form Authorization To Disclose Health Information. An authorization permits, but does not require, a DHS agency to disclose individually identifiable health information.

4009.3.2 Exceptions where limited uses or disclosures are allowed without authorization, to the extent not prohibited or otherwise limited by federal or state requirements applicable to the program or activity

4009.3.2.1 DHS clients or participants may access their own information, with certain limitations.

4009.3.2.2 DHS may use or disclose information without an individual's authorization if the law requires such use or disclosure, and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

4009.3.2.3 Internal communication within DHS is permitted without individual authorization, in compliance with the DHS Policy Minimum Necessary Information.

Note: Alcohol and drug, mental health, and vocational rehabilitation records disclosure may be limited to particular program areas named on the authorization

form. If such a limitation is noted on the authorization form, disclosure is limited to the parties named.

4009.3.2.4 DHS may disclose information without authorization to another covered entity or a health care provider for the payment activities of the entity that receives the information.

4009.3.2.5 DHS may disclose information without authorization to another entity covered by federal HIPAA law and rules for the health care activities of that entity, if:

- A. Both that entity and DHS has or has had a relationship with the individual who is the subject of the information.
- B. The information pertains to such relationship; and
- C. The disclosure is for the purpose of:
 - 1. Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or
 - 2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improvement their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or
 - 3. Detecting health care fraud and abuse or for compliance purposes.

4009.3.2.6 DHS may use or disclose psychotherapy notes:

- A. Use by the originator of the psychotherapy notes, for treatment purposes.
- B. In training programs where students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
- C. When a health oversight agency uses or discloses in connection with oversight of the originator of the psychotherapy notes; or
- D. To the extent authorized under state law to defend DHS in a legal action or other proceeding brought by the individual.
- E. Investigations by the Secretary of the US Department of Health and Human Services;

- F. Coroners and Medical Examiners;
- G. Institution Review Board or Privacy Board approval for waiver of authorization for research purposes.

Note: Questions regarding the agency's authority to disclose psychotherapy notes without a valid authorization should be referred to the DHS Privacy Officer.

4009.3.2.7 DHS may disclose information for purposes of payment, treatment, and health care operations.

4009.3.2.8 If DHS has reasonable cause to believe that a child is a victim of abuse or neglect, DHS may disclose protected information to appropriate governmental authorities authorized by law to receive reports of child abuse or neglect (including reporting to DHS protective services staff, if appropriate). If DHS receives information as the child protective services agency, DHS is authorized to use and disclose the information consistent with its legal authority.

A. Reports and records compiled are confidential and are not accessible for public inspection. However if DHS receives the information, DHS will:

1. Use and disclose the information consistent with its legal authority as a child protective services agency;
2. Subject to applicable law, DHS may make available records and reports to:
 - a. Any law enforcement agency or a child abuse registry in any other state for the purposes of additional investigations of child abuse;
 - b. Any physician, at the request of the physician, regarding any child brought to the physician or coming before the physician for examination, care or treatment;
 - c. Attorneys of record for the child or child's parent or guardian in any juvenile court proceeding;
 - d. Citizen review boards established by the Judicial Department for the purpose of periodically reviewing the status of children, youths and youth offenders under the jurisdiction of the juvenile court. Citizen review boards may make such records available to participants in case review;
 - e. A court appointed special advocate (CASA) in any juvenile Court proceeding in which it is alleged that a child has been abused or neglected; and
 - f. The Child Care Division for certifying, registering or otherwise regulating childcare facilities.

- B. Consistent with applicable law, DHS may make reports and records available to any person, administrative hearings officer, court, agency, organization or other entity when the department determines that such disclosure is necessary to:
 - 1. Administer its child welfare services and is in the best interests of the affected child;
 - 2. The disclosure is necessary to investigate, prevent or treat child abuse and neglect; or
 - 3. Protect children from abuse and neglect.
- C. DHS may not disclose the names, addresses or other identifying information about the person who made the report.

4009.3.2.9 DHS may use or disclose information without the written authorization of the individual if DHS has reasonable cause to believe that an adult is a victim of abuse or neglect (elder abuse, nursing home abuse, or abuse of the mentally ill or developmentally disabled), DHS may disclose protected information to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse or neglect:

- A. If the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or
- B. If the individual agrees to the disclosure, either orally or in writing; or
- C. When DHS staff, in the exercise of professional judgment and in consultation with appropriate DHS supervisor, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
- D. When the individual is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:
 - 1. The protected information being sought is not intended to be used against the individual, and
 - 2. An immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- E. When DHS staff make a disclosure permitted above, DHS must promptly inform the individual that such a report has been or will be made, except if:
 - 1. DHS staff, in the exercise of professional judgment and in consultation with appropriate DHS supervisor, believes informing the individual would place the individual or another individual at risk of serious harm; or

2. DHS staff would be informing a personal representative and DHS staff reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the individual, as determined by DHS staff, in the exercise of professional judgment and in consultation with appropriate DHS supervisor.

4009.3.2.10 DHS may use or disclose information without the written authorization of the individual for the purpose of carrying out duties in its role as a health oversight agency, DHS does not need to obtain an individual's authorization to lawfully receive, use or disclose individual information for oversight activities authorized by law.

- A. DHS may disclose information to a health oversight agency to the extent the disclosure is not prohibited by state or federal law for its oversight activities of:
 1. The health care system
 2. Government benefit programs for which the information is relevant to eligibility;
 3. Entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards; or
 4. Entities subject to civil rights laws for which the information is necessary for determining compliance.
- B. **Exception:** a health oversight activity for which information may be disclosed does **not** include an investigation or other activity of which the individual is the subject **unless** the investigation or other activity is directly related to:
 1. The receipt of health care;
 2. A claim to recover public benefits related to health; or
 3. Qualifying for or receiving public benefits or services based on the health of the individual.
- C. If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered a health oversight activity for purposes of this section.
- D. When DHS is acting as a health oversight agency, DHS may use information for health oversight activities as permitted under this section.

4009.3.2.11 DHS may use or disclose information without the written authorization for the individual when DHS discloses information in a judicial or administrative proceeding subject to the following:

- A. DHS must follow any procedures for responding to subpoenas, discovery requests, or other requests for documents that DHS may have regarding an individual; DHS must not ignore any subpoena or other legal document.
 - 1. In general, DHS will respond by appearing before the Court to explain that the information is confidential, or by filing a legal response through the Department of Justice. DHS will not disclose any confidential information in a court proceeding in which DHS is not a party except as required by law or by a court order
 - 2. An administrative hearings officer or administrative law judge lacks legal authority, under Arkansas law, to require or authorize DHS to disclose information about an individual that is confidential under federal or state law. DHS staff should work with hearing officers to ensure that protective orders are used when appropriate in contested case hearings to prevent authorized uses and disclosures of information.
 - 3. DHS staff will refer any questions or concerns regarding what is required by law, or by a court order, to the DHS Privacy Officer, who may then consult with the Department of Justice to resolve the question.
- B. DHS may use or request information to investigate a grievance or appeal made to DHS about an individual's eligibility or right to benefits or services.
 - 1. Pursuant to applicable laws and rules, DHS may use or disclose information that DHS has compiled on its own or has received from external sources.
 - 2. That information may be reviewed by DHS staff and legal counsel, the providers or health plan involved in the service or action, and may be provided to a hearing officer, to assist DHS in making a decision about the appeal or grievance.
- C. If DHS is sued or if a suit is filed on behalf of DHS, the Department of Justice will address or respond to legal issues related to the use and disclosure of information. DHS will identify confidentiality issues for discussion with the assigned legal counsel, in consultation with the DHS Privacy Officer.
- D. If a court orders DHS to conduct a mental examination (such as in accordance with state law), or orders DHS to provide any other report or valuation to the court such examination, report or evaluation shall be deemed to be "required by law" for purposes of HIPAA, and DHS staff will comply with the court order.

- E. If DHS has obtained information in performing its duties as a health oversight agency, public health authority, protective service entity, or public benefit program, nothing in this section supersedes DHS policies that otherwise permit or restrict uses or disclosures. For example, if DHS has obtained individual patient information as a result of an oversight action against a provider, DHS may lawfully use that patient information in a hearing consistent with the other confidentiality requirements applicable to that program, service or activity.
- F. In any case in which federal or state law prohibits or restricts the use or disclosure of information in an administrative or judicial proceeding, DHS shall assert the confidentiality of such confidential information, consistent with DHS policies applicable to the program, service or activity, to the presiding officer at the proceeding. A HIPAA-authorized protective order may not be sufficient to authorize disclosure if it does not address other applicable confidentiality laws.

4009.3.2.12 DHS may use or disclose information without the written authorization of the individual for law enforcement purposes unless federal or state law prohibits such disclosure.

- A. DHS may disclose information when reporting certain types of wounds or other physical injuries.
- B. DHS may disclose information in compliance with, and limited to the relevant specific requirements of:
 - 1. A court order or warrant, summons or subpoena issued by a judicial officer;
 - 2. A grand jury subpoena; or
 - 3. An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that the information is relevant, material, and limited to a legitimate law enforcement inquiry.

Note: Follow DHS procedures for responding to subpoenas, Discovery requests, or other requests for documents that DHS may have regarding an individual. Do not ignore any subpoena or other legal document. **Exception:** Information regarding mental health, alcohol or drug treatment, and vocational rehabilitation services can be disclosed only on the basis of a court order.

- C. DHS may disclose limited protected information upon request of a law enforcement official without authorization for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that the information DHS may thus disclose is limited to:
 - 1. Name and address;
 - 2. Date and place of birth;

3. Social security number;
4. ABO blood type and Rh factor;
5. Type of injury;
6. Date and time of treatment;
7. Date and time of death if applicable; and
8. A description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos. In cases of criminal court commitments, a photograph may be provided.

Exception: DHS may not disclose, for purposes of identification or location, protected health information related to the subject's DNA or DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissues, unless ordered to do so by a court or a court approved search warrant.

- D. DHS may disclose protected information upon request to a law enforcement official about an individual who is or is suspected to be the victim of a crime, if:
 1. DHS is otherwise authorized by law to disclose that information for purposes of an abuse reporting law or for public health or health oversight purposes; or
 2. The individual agrees to the disclosure, either orally or in writing; or
 3. DHS is unable to obtain the individual's agreement due to incapacity or emergency circumstance, if:
 - a. The law enforcement official represents that such information is needed to determine whether a violation of law by someone other than the victim has occurred and such information is not intended for use against the victim;
 - b. The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - c. DHS determines that the disclosure is in the best interests of the individual.
- E. DHS may disclose protected information to a law enforcement official about an individual who has died, for the purpose of alerting law enforcement of the death, if DHS suspects that death may have resulted from criminal conduct.
- F. DHS may disclose protected information to a law enforcement official if DHS believes in good faith that the information constitutes evidence of criminal conduct on DHS premises.

- G. Necessary for law enforcement authorities to identify or apprehend an individual:
 - 1. Because of a statement by a person admitting participation in a violent crime that DHS reasonably believes may have caused serious harm to the victim; or
 - 2. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.
- H. DHS may disclose to a coroner or medical examiner, for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.
- I. DHS may disclose individual information without authorization to funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent. DHS may also disclose such information prior to, and in reasonable anticipation of, the death.
- J. DHS may disclose individual information without authorization to Organ procurement organizations or other entities engaged in procuring, banking, or transplantation of cadaver organs, eyes, or tissue, for the purpose of facilitating transplantation.
- K. To avert a serious threat to health or safety, DHS may disclose individual information without authorization if:
 - 1. DHS believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
 - 2. The report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
- L. DHS may disclose individual information without authorization for other specialized government functions, including authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.
- M. DHS may disclose limited information without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of individuals or other inmates.
- N. In case of an emergency, DHS may disclose individual information without authorization to the extent needed to provide emergency treatment.
- O. The Family Educational Rights and Privacy Act (FERPA) and state Law applicable to student records governs DHS access to, use, and disclosure of student records.

4009.3.3 Client or Participant’s authorization that is not required if they are informed in advance and given a chance to object:

4009.3.3.1 In limited circumstance, DHS may use or disclose an individual’s information without authorization if:

- A. DHS informs the individual in advance and the person has been given an opportunity to object.
- B. Unless otherwise protected by law, DHS may orally inform the individual and obtain and document the individual’s oral agreement.

4009.3.3.2 Disclosures are limited to disclosure of health information to a family member, other relative, or close personal friend of the individual, or any other person named by the individual.

Note: For individuals receiving alcohol and drug, mental health, or vocational rehabilitation services, oral permission is not sufficient and written authorization is required.

4009.3.3.3 Oral permission to use or disclose information for the purposes described in subsections (a) of this section is not sufficient when the individual is referred to or receiving substance abuse treatment services or mental health treatment services, where written authorization for the treatment program to make such disclosures is required.

4009.3.4 Routine and Recurring Disclosure of an Individual’s Information:

For the purposes of this policy, a “routine and recurring” means the disclosure of records outside DHS, without the authorization of the individual, for a purpose that is compatible with the purpose for which the information was collected. The following identifies several examples of uses and disclosures that DHS has determined to be compatible with the purposes for which information is collected.

4009.3.4.1 DHS will not disclose an individual’s entire medical record unless the request specifically justifies why the entire medical record is needed.

4009.3.4.2 Routine and recurring uses include disclosures required by law. For example, a mandatory child abuse report by a DHS employee would be a routine use.

4009.3.4.3 If DHS deems it desirable or necessary, DHS may disclose information as a routine and recurring use to the Department of Justice for the purpose of obtaining its advice and legal services.

4009.3.4.4 When federal or state agencies – such as the DHHS Office of Civil Rights, the DHHS Office of Inspector General, the State of Arkansas Medicaid Fraud Unit, or the Arkansas Secretary of State – have the legal authority to require DHS to produce records necessary to carry out audit or oversight of DHS programs or activities, DHS will make such records available as a routine and recurring use.

- 4009.3.4.5 When the appropriate DHS official determines that records are subject to disclosure under the Arkansas Freedom of Information Act, DHS may make the disclosure as a routine and recurring use.

4009.3.5 Non-routine Disclosure of an Individual's Information

- 4009.3.5.1 For the purpose of this policy, “non-routine disclosure” means the disclosure of records outside DHS that is not for a purpose for which it was collected.
- 4009.3.5.2 DHS will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor.
- 4009.3.5.3 Requests for non-routine disclosures must be reviewed on an individual basis in accordance with the criteria set forth in the Procedure section.

4009.3.6 Re-disclosure of an Individual's Information

- 4009.3.6.1 Unless prohibited by State and Federal laws, information held by DHS and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by DHS policy. Whether or not the information remains protected depends on whether the recipient is subject to federal or state privacy laws, court protective orders or other lawful process.
- 4009.3.6.2 Vocational Rehabilitation and Alcohol and Drug Rehabilitation information: Federal regulations (42 CFR part 2 and 34 CFR 361.38) prohibit DHS from making further disclosure of vocational rehabilitation and alcohol and drug rehabilitation information without the specific written authorization of the individual to whom it pertains.
- 4009.3.6.3 Arkansas law and administrative rule prohibits further disclosure of HIV information.
- 4009.3.6.4 Arkansas law and administrative rule prohibits further disclosure of Genetics information without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical information is not sufficient for this purpose.
- 4009.3.6.5 Arkansas law places restrictions on re-disclosure of information regarding clients of publicly funded mental health or developmental disability providers.

4009.3.7 Revocation of Authorization

- 4009.3.7.1 An individual can revoke an authorization at any time. The authorization must state that a client has the right to revoke the authorization at any time, except to the extent that the DHS agency has already taken action based the authorization. The authorization form must include instructions on how the client may revoke an authorization.

4009.3.7.2 Any revocation must be in writing and signed by the individual or their personal representative. Page 2 of the Authorization to Disclose Health Information contains the Revocation Section. This section must be completed when revocation of the authorization to disclose protected health information is requested. Legible faxed copies of this form are permissible.

Exception: alcohol and drug treatment participants may orally revoke authorization to disclose information obtained from alcohol and drug treatment programs. Oral authorizations must be documented and maintained in the individual's record.

4009.3.7.3 When the signed revocation is received, page 2 of the Authorization to Disclose Health Information must be filed on top of page 1.

4009.3.7.4 Upon receipt of the written revocation or documentation of oral revocation (as noted in Exception), DHS shall immediately cease release of protected health information.

4009.3.7.5 No such revocation shall apply to information already released while the authorization was valid and in effect.

4009.3.8 Verification of Individuals Requesting Information

4009.3.8.1 If the DHS staff member fulfilling the request does not know the person requesting information, no information may be disclosed without verification of the identity of the person requesting the information

4009.3.8.2 If the requestor is a Provider, they will need to supply their provider identification number and/or telephone number for call back.

4009.3.8.3 For all other requestors, reasonable evidence should be supplied in the form of the following:

- A. Identification badge
- B. Driver's license
- C. Written statement of identity on agency letterhead; or
- D. Similar proof

4009.3.9 Denial of Requests for Information

Unless an individual has signed an authorization, or the information about the individual can be disclosed pursuant to this Policy, DHS shall deny any request for individual information.

4009.4.0 DHS Standard Authorization

4009.4.1 All DHS agencies shall utilize the standard authorization form, " Authorization to Disclose Health Information", that contains the elements necessary to be considered a valid authorization. The standard authorization form is written in plain and simple language that a client or personal representative can easily read and understand.

The standard authorization shall be made available in languages understood by a substantial number of clients served by each agency. At a minimum, the department shall ensure the standard authorization in Spanish translation is available to DHS agencies. Braille authorization forms shall be available to clients who are blind from the Division of Services for the Blind, upon request for such format.

4009.4.2 DHS divisions and offices may add their agency's identification information and form number to the standard form; however, any other alterations to the standard form must be prior approved by the DHS Privacy Officer, who is responsible for the development and maintenance of the DHS standard authorization form. Each agency is responsible for printing its own authorization forms.

4009.5.0 When an Authorization is required

4009.5.1 Except as otherwise permitted or required by law and consistent with these policies, DHS shall obtain a completed and signed authorization for release of information from the individual, or the individual's personal representative, before obtaining or using information about an individual from a third party or disclosing any information about the individual to a third party.

4009.5.2 A signed authorization is required in the following situations:

4009.5.2.1 Prior to an individual's enrollment in a DHS administered health plan

4009.5.2.2 If necessary for determining eligibility or enrollment

4009.5.2.3 For the use and disclosure of psychotherapy notes

4009.5.2.4 For disclosures to an employer for use in employment-related determinations

4009.5.2.5 For research purposes unrelated to the individual's treatment

4009.5.2.6 For any purpose in which state or federal law requires a signed Authorization

4009.6.0 Valid Authorization

Requests for Disclosure of Protected Health Information (PHI) must be made utilizing DHS Authorization To Disclose Health Information Form. If requests for PHI are received on any other form, the request will be returned to the requesting entity with a copy of the appropriate form.

4009.6.1 Uses and disclosures must be consistent with what the individual has authorized on a signed authorization form.

4009.6.2 An authorization must be voluntary. DHS may not require the individual to sign an authorization as a condition of providing treatment services, payment for health care services, enrollment in a health plan, or eligibility for health plan benefits, except as noted under Conditioning of an Authorization.

4009.6.3 Each authorization for use or disclosure of an individual's information must be fully completed jointly by the staff member and the individual, whenever possible, with the staff worker taking reasonable steps to ensure that the individual understands why the information is to be used or released.

4009.6.4 DHS staff will use the approved DHS authorization forms (Authorization to Disclose Health Information).

4009.6.5 A valid authorization must contain the following information:

4009.6.5.1 A description of the information to be used or disclosed, that identifies the purpose of the information in a specific and meaningful fashion;

4009.6.5.2 The name or other specific information about the person(s), classification of persons, or entity (i.e., DHS or specified DHS program) authorized to make the specific use or disclosure;

4009.6.5.3 The name or other specific identification of the person(s), classification of persons, or entity to whom DHS may make the requested use or disclosure;

4009.6.5.4 A description of each purpose of the requested disclosure (the statement at the request of the client" is a sufficient description of the purpose when a client initiates the authorization and does not, or elects not to, provide a statement of the purpose);

4009.6.5.5 An expiration date or event that relates to the client or the purpose of the use or disclosure. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:

A. The statement "end of the research study" or similar language is sufficient if the authorization is for use or disclosure of individually identifying health information for research.

B. The statement "none" or similar language is sufficient if the authorization is for the agency to use or disclose individually identifying health information for the creation and maintenance of a research database or research repository.

4009.6.5.6 Signature of the client and the date of the signature. If a client's personal representative signs the authorization form, a description of the personal representative's authority to act on behalf of the client must also be provided including a copy of the legal court document (if any) appointing the personal representative, must also be provided.

4009.6.6 An original authorization form is preferred for disclosure of individually identifiable health information; however, a clear and legible photocopy or facsimile is acceptable.

4009.7.0 Invalid Authorization

An Authorization shall be considered invalid if the document has any of the following deficiencies:

- A. The expiration date has passed or the expiration event is known to have occurred.
- B. The Authorization form is not completely filled out.
- C. The Authorization form does not contain the core elements of a valid authorization.
- D. The Authorization is known to have been revoked.
- E. Any information recorded on the Authorization form is known to be false.
- F. An Authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

4009.8.0 Compound Authorization

- 4009.8.1** An authorization for disclosure of individually identifiable health information shall not be combined with any other written legal permission from the client (e.g., Consent for Treatment, Assignment of Benefits); however, research studies that include treatment may combine authorizations for the same research study, including consent to participate in the study.
- 4009.8.2** An authorization for disclosure of psychotherapy notes may not be combined with any other authorization.
- 4009.8.3** An authorization that specifies a condition for the provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be combined with any other authorization.
- 4009.8.4** An authorization that is required for enrollment in a health plan or to determine eligibility for benefits of the health plan cannot be combined with a voluntary authorization. A required authorization and a voluntary authorization must be separate documents, signed separately.

4009.9.0 Conditioning of Authorization

The provision of treatment, payment, enrollment in a health plan or eligibility for benefits shall not be conditioned on whether or not a client signs an authorization form, except as follows:

- 4009.9.1** The provision of research-related treatment can be conditioned on a client authorizing the use or disclosure of individually identifiable health information for such research;
- 4009.9.2** Provision of health care solely for the purpose of creating individually identifiable health information for disclosure to a third party (E.g., physical exam for life insurance); or
- 4009.9.3** Prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations and the authorization is not for disclosure of psychotherapy notes.

- 4009.9.3.1 Before providing research-related treatment, a DHS health care provider may condition the individual to sign an authorization for the use or disclosure of health information for such research; or
- 4009.9.3.2 Before enrolling the individual in a DHS health plan, DHS can condition the individual to sign an authorization if needed to help determine the applicant's eligibility for enrollment and the authorization is not for a use or disclosure of psychotherapy notes; or
- 4009.9.3.3 DHS and its contracted health care providers can require the individual to sign an authorization before providing health care that is solely for the purpose of creating protected health information for disclosure to a third party. For example, in a juvenile court proceeding where a parent is required to obtain a psychological evaluation by DHS, the evaluator may, as a condition of conducting the evaluation, require the parent to sign an authorization to release the evaluation report (but not the underlying psychotherapy notes) to DHS.

4009.10.0 Retention Period

DHS must document and retain each signed Authorization Form for a minimum of six years.

4009.11.0 Contractor Authorizations

The authorization requirements contained in this policy also apply to contractors who perform a service for or on behalf of a DHS agency. Such Contractors are limited to those disclosures permitted in an agreement with the agency. Contractors are responsible for ensuring that policy requirements are enforced with any sub-contractors they may use.

4009.12.0 Department Contact

Any questions concerning DHS Policy Number 4009 should be directed to:

DHS Office of Chief Counsel
Post Office Box 1437/Slot S260
Little Rock, Arkansas 72203-1437
Telephone: (501) 682-8934

ARKANSAS DEPARTMENT OF HUMAN SERVICES

Access to Records Request Form

(For use by DHS clients requesting access to records.)

Client Name: _____ Client ID #: _____
Mailing Address: _____ Date of Birth: _____
_____ Case Head: _____
Record Holder: _____ Type of Record: _____
Location of Record: _____

If you are asking for access to your records or the records of a person for whom you are the custodian or personal representative, please consider the following:

- You may ask to access, look at or get information that is in DHS records.
- DHS cannot give you access to psychotherapy notes.
- DHS may deny you access to information if someone other than a health care provider gave it to DHS. Such information cannot be disclosed under the Arkansas Freedom of Information Act.
- You will have an answer to your request within 30 days. If the information is not at this location, you will have an answer within 60 days. If there are delays in getting you the answer, you will be told. The delay will not be more than 30 days. You will receive an answer in writing.

I am asking for access to information for myself or for someone for whom I am the custodian or legal guardian for the following time period:

From: _____ To: _____
Print Name: _____

Signature Date

FOR DHS USE	
<input type="checkbox"/> Approved	<input type="checkbox"/> Denied
<input type="checkbox"/> Delayed	
Comments: _____	

_____	_____
DHS Representative Signature	Date

(See other side for client rights information)

ARKANSAS DEPARTMENT OF HUMAN SERVICES

Access to Records Request Form

(For use by DHS clients requesting access to records.)

Your Right to Access Information:

- You have a right to request access, look at or get information about yourself or for someone who is in your custody or for whom you are the personal representative that is in DHS records.
- You may be charged a fee, if you have accessed the same information within the past year.
- Your request may be denied if professionals involved in the case believe that access to the information could be harmful to you or others.
- The reviewer must decide, within a reasonable time, whether to approve or deny your request. You will get an answer in writing. The answer will include the reason for the decision.

You have a right to file a privacy complaint:

Individuals can file privacy complaints with either DHS or with the U.S. Department of Health and Human Services, Office for Civil Rights.

Privacy complaints may be directed to any of the following:

Arkansas Department of Human Services

DHS Privacy Official
P.O. Box 1437 Mail Slot S201
Little Rock, Arkansas 72203-1437
Phone: 501-682-8650
Email: Privacyofficial@mail.state.ar.us

U.S. Department of Health and Human Services, Office for Civil Rights

Medical Privacy, Complaint Division
200 Independence Avenue, SW
HHH Building, Room 509H
Washington, D.C. 20201
Phone: 866-627-7748
TTY: 866-788-4989
Email: www.hhs.gov/ocr

This document is available in other languages and alternate formats that meet the guidelines for the Americans with Disabilities Act (ADA). Contact DHS at:
Phone 501-582-8920, TDD 501-682-8933 or Fax 501-682-8884.

ARKANSAS DEPARTMENT OF HUMAN SERVICES
Termination of Alternate Delivery of PHI

Date

Mailing Address

Mailing Address

Mailing Address

Re: *HR#*

Dear Mr./Ms. *Name*

Your request for alternate delivery of your protected health information has been terminated. Attempts to deliver your protected health information in the manner that you requested have been unsuccessful as indicated below:.

- ☐ Mail sent to the alternate address that you provided has been returned as undeliverable.
- ☐ The telephone number to your facsimile machine has been disconnected.
- ☐ There is no operable facsimile machine at the telephone number that you provided for delivery.
- ☐ E-mail sent to the address that you provided has been returned as undeliverable.
- ☐ Other reason as follows: _____
-
-

You have a right to file a privacy complaint concerning the termination of alternate delivery of your protected health information. Individuals can file privacy complaints with either DHS or with the U.S. Department of Health and Human Services, Office for Civil Rights. Privacy complaints may be directed to any of the following:

DHS Privacy Official
Arkansas Department of Human Services
PO Box 1437, Slot S201
Little Rock, Arkansas 72201-1437
Phone: 501-682-8650
Fax: 501-682-6836
TDD: 501-682-7958
Email: PrivacyOfficial@mail.state.ar.us

U.S. Department of Health and Human Services
Office for Civil Rights
Medical Privacy, Complaint Division
200 Independence Avenue, SW
HHH Building, Room 509H
Washington, D.C. 20201
Phone: 866-627-7748
TTY: 886-788-4989 Email: www.hhs.gov/ocr

Sincerely,

DHS Representative Signature

Title

ARKANSAS DEPARTMENT OF HUMAN SERVICES

COMPLAINT

Violation by DHS of HIPAA Privacy Rights

1. The person filing this Complaint (the Complainant) is: (check the appropriate box below)

Complainant:

- ☐ The DHS Client whose privacy rights were violated (Client fills out Number 2 below, skips Number 3 below, and continues with Number 4 below).
- ☐ The Personal Representative of the DHS client whose privacy rights were violated (Personal Representative fills out the information in **both** Number 2 and Number 3 below and continues with Number 4 below)

2. Information about DHS Client (Client)

DHS Client Information: (this is the person whose privacy rights were violated)

Name (printed): _____

Mailing Address: _____

Telephone Numbers:

Work: _____ Home: _____ Other: _____

Date of Birth: _____ ID Number: _____ Record Number: _____

3. Information about DHS Client's Personal Representative (if Personal Representative is filing this Complaint).

Personal Representative Information:

Name (printed): _____

Mailing Address: _____

Telephone Numbers:

Work: _____ Home: _____ Other: _____

Relationship to Client: _____

Please describe below your authority to represent this Client and attach documentation of your authority to represent this client.

ARKANSAS DEPARTMENT OF HUMAN SERVICES

COMPLAINT

Violation by DHS of HIPAA Privacy Rights

4. The Complainant hereby submits this Complaint to the office of the DHS Privacy Officer.

DHS Privacy Officer
Department of Human Services
P.O. Box 1437, Mail Slot S201
Little Rock, Arkansas 72203-1437

5. Complainant reserves the right to file a separate complaint on the same set of facts presented in this Complaint with the U.S. Department of Health and Human Services Office for Civil Rights.

U.S. Department of Health and Human Services
Office for Civil Rights, Medical Privacy, Complaint Division
200 Independence Avenue, SW
HHH Building, Room 509H
Washington, D.C. 20201

Phone: 1 866 627 7748 TTY: 886-788-4989 Email: www.hhs.gov/ocr

6. DHS violated Client's privacy rights guaranteed under the federal law entitled "Health Insurance Portability and Accountability Act of 1996" (HIPAA) and the regulations promulgated pursuant to that law.

Identity the person who violated Client's privacy rights, and the date it occurred:

- A. DHS Office that violated Client's privacy rights: _____
B. Person who violated Client's privacy rights (if known): _____
C. Date Client's rights were violated (approximate date is OK): _____

NOTE: This Complaint must be filed within 180 days from the time Client or Client's Personal Representative knew or should have known that Client's HIPAA privacy rights were violated.

Description of the privacy rights violation:

Describe how Client's privacy rights were violated: (attach additional sheets if needed)

ARKANSAS DEPARTMENT OF HUMAN SERVICES

COMPLAINT

Violation by DHS of HIPAA Privacy Rights

7. Complainant requests the following relief from DHS:
 - A. That DHS investigate the allegations made in this Complaint; and
 - B. That DHS deliver to Complainant a written report of the results of the investigation not more than sixty (60) days from the date DHS receives this Complaint; and
 - C. That DHS correct the violations of Client's rights; and
 - D. That DHS take action to prevent similar violations in the future.
8. The Complainant affirms that the information stated in this Complaint is true and correct to the best of Complainant's information, knowledge and belief.

Note: Only the Complainant, who is either the Client or the Client's Personal Representative, signs this Complaint.

Client's Name (Printed)

Client's Signature

Date

OR:

Personal Representative's Name (Printed)

Personal Representative's Signature

Date

ARKANSAS DEPARTMENT OF HUMAN SERVICES

Confidential Communications

(For requests to receive protected health information via an alternate means or to receive protected health information at an alternate location.)

Client Name: _____ Client ID #: _____
Mailing Address: _____ Date of Birth: _____
_____ Case Head: _____
Record Holder: _____ Date of Request: _____
Location of Record: _____

☐ I am a client or a legal representative of a client of the Department of Human Services.

☐ I am an employee or legal representative of an employee of the Department of Human Services.

To maintain confidentiality of health information that I may request from the Department of Human Services, I request that all protected health information concerning myself or any other individuals that I am legally entitled to represent be sent to me as follows:

1. By mail to the following address: _____
2. By mail, using a plain envelope with no return address, to the following address: _____
3. By facsimile (FAX) to the following phone number: _____
4. By e-mail to the following address*: _____
5. By other means as follows: _____

* If e-mail is the selected mode of delivery for protected health information, the Department of Human Services cannot guarantee the security of the information transmission.

I understand that the Department of Human Services must accommodate reasonable requests for alternate delivery of my protected health information to me. I also understand that DHS may terminate this accommodation at my request or if the delivery method that I have specified does not prove to be an effective means for delivery of my protected health information.

Signature of Client/Employee or Client/Employee's Legal Representative

Date

FOR DEPARTMENT OF HUMAN SERVICES INTERNAL USE ONLY

Date Request Received _____

☐ Alternate Delivery Means Annotated in record.

DHS Representative Signature

Date

Copy To (Privacy Officer and all other Divisions/Office who hold client/employee PHI):

- ☐ DHS Privacy Officer ☐ DHS Office of Administrative Services ☐ DHS Office of Chief Council
☐ DHS Office of Fiscal Management ☐ DHS Office of Systems & Technology ☐ Division of Aging and Adult Services
☐ Division of Child Care and Early Childhood Education ☐ Division of Children and Family Services
☐ Division of County Operations ☐ Division of Developmental Disabilities Services ☐ Division of Medical Services
☐ Division of Mental Health Services ☐ Division of Services for the Blind ☐ Division of Volunteerism
☐ Division of Youth Services

ARKANSAS DEPARTMENT OF HUMAN SERVICES

Confidential Communications

(For requests to receive protected health information via an alternate means or to receive protected health information at an alternate location.)

Confidential Communications

- You have the right to request that protected health information held by the Department of Human Services be delivered to you in a confidential manner.
- When you request information from the Department of Human Services, it will normally be mailed to you by first class mail to the current address reflected in your record.
- By completing this form, you may request that the Department of Human Services deliver your protected health information by a different method such as facsimile or e-mail or you may request that the Department of Human Services deliver your protected health information to a different address or with special handling.
- The Department of Human Services must permit clients to request and must accommodate reasonable requests by clients to receive communications of protected health information (PHI) from DHS by alternative means or at alternative locations.
- The Department of Human Services will make reasonable accommodations to deliver your protected health information to you by the means or to the location that you have requested until you terminate the request or the until the Department determines that the method of delivery is unreliable.

You have a right to file a privacy complaint concerning the termination of alternate delivery of your protected health information. Individuals can file privacy complaints with either DHS or with the U.S. Department of Health and Human Services, Office for Civil Rights. Privacy complaints may be directed to any of the following:

Arkansas Department of Human Services
Privacy Officer
PO Box 1437, Slot S201
Little Rock, Arkansas 72201-1437
Phone: 501-682-8650
Fax: 501-682-6836 Email: PrivacyOfficer@mail.state.ar.us

U.S. Department of Health and Human Services, Office for Civil Rights

Medical Privacy, Complaint Division
200 Independence Avenue, SW
HHH Building, Room 509H
Washington, D.C. 20201
Phone: 866-627-7748
TTY: 886-788-4989 Email: www.hhs.gov/ocr

<p>This document is available in other languages and alternate formats that meet the guidelines for the Americans with Disabilities Act (ADA). Contact DHS at: Phone 501-582-8920, TDD 501-682-8933 or Fax 501-682-8884.</p>
--